Corso di Laurea Triennale in **Matematica** - a.a. 2020/2021

programma di **ALGEBRA 1** (8 CFU)

prof. **Fabio Gavarini**

1 – INSIEMI, RELAZIONI, APPLICAZIONI

Insiemi, sottoinsiemi; insieme delle parti di un insieme. Unione, intersezione, differenza, differenza simmetrica, prodotto cartesiano di insiemi; complementare di un sottoinsieme.

Corrispondenze tra insiemi; relazioni, funzioni (o "applicazioni"). Famiglie di oggetti in un insieme.

Partizioni di un insieme; insieme quoziente e proiezione canonica associati a una partizione.

Funzioni iniettive, suriettive, biiettive. Composizione di funzioni; funzioni invertibili, funzione inversa; caratterizzazioni delle funzioni invertibili; permutazioni di un insieme. Funzioni caratteristiche su un insieme; biiezione tra funzioni caratteristiche e insieme delle parti.

Relazioni (binarie); casi speciali; relazioni di preordine, d'ordine, di equivalenze. Classi di equivalenza, rappresentanti; insieme quoziente e applicazione canonica. Biiezione tra equivalenze in X e quozienti di X. L'equivalenza associata a un'applicazione. Il *Teorema Fondamentale delle Applicazioni*.

2 – IL SISTEMA DEI NUMERI NATURALI

Il Sistema dei Numeri Naturali $\mathbf{N}$: assiomi di Peano, esistenza, unicità. Principio di Induzione Semplice, Principio di Induzione forte, Principio del minimo. Metodi di dimostrazione per induzione.

Somma, prodotto e ordinamento per i naturali. Divisione con resto tra numeri naturali.

Scrittura posizionale dei numeri naturali; numerazioni in base qualsiasi, cambiamenti di base.

3 – CARDINALITÀ

Insiemi equipotenti: cardinalità di un insieme, numeri cardinali; insiemi finiti e infiniti; ordine tra numeri cardinali; cardinalità del numerabile. Caratterizzazione degli insiemi infiniti.

Primo Teorema ("diagonale") di Cantor. *Secondo Teorema di Cantor* (sulla cardinalità dell'insieme delle parti). Cardinali infiniti superiori; l'ipotesi generalizzata del continuo. La distribuzione (rispetto all'ordine) dei numeri cardinali. L'insieme $\mathbf{R}$ dei numeri reali ha la cardinalità del continuo (cenni).

4 – INSIEMI CON OPERAZIONI

Insiemi con una operazione (=gruppoidi); semigruppi, monoidi, gruppi; elementi speciali. Gli invertibili in un monoide M formano un gruppo $U(M)$. Insiemi con più operazioni.

(Omo)morfismi di gruppoidi. Il *Teorema di Cayley per Semigruppi*; il caso speciale dei monoidi.

Prodotto diretto di gruppoidi; gruppoidi di funzioni (a valore in un gruppoide).

Relazioni compatibili in un gruppoide; gruppoidi quoziente. L'equivalenza associata ad un morfismo di gruppoidi è compatibile (nel gruppoide dominio), e l'applicazione canonica è un (epi)morfismo dal gruppoide al gruppoide quoziente. Il *Teorema Fondamentale di Omomorfismo per Gruppoidi*.

Gruppoidi cancellativi. Costruzione del gruppo associato ad un gruppoide commutativo cancellativo; esempi: $(\mathbf{Z};+)$ - associato a $(\mathbf{N};+)$ - $(\mathbf{Q}_+;\cdot)$ - associato a $(\mathbf{N}_+;\cdot)$ - e $(\mathbf{Q}^*;\cdot)$ - associato a $(\mathbf{Z}^*;\cdot)$.

5 – I NUMERI INTERI

Costruzione di $(\mathbf{Z};+)$ come gruppo associato al semigruppo commutativo cancellativo $(\mathbf{N};+)$. Somma, prodotto, ordinamento e valore assoluto in $\mathbf{Z}$: definizione e proprietà fondamentali.

Divisibilità in $\mathbf{Z}$: elementi primi, elementi irriducibili. Ogni elemento primo è irriducibile. *M.C.D.* e *m.c.m.* in $\mathbf{Z}$. Divisione euclidea (con resto) in $\mathbf{Z}$. Esistenza del *M.C.D.* in $\mathbf{Z}$, e identità di Bézout; calcolo tramite l'algoritmo euclideo. Equazioni diofantee; criterio di risolubilità, algoritmo di risoluzione.

In $\mathbf{Z}$ ogni elemento irriducibile è primo. Il *Teorema Fondamentale dell'Aritmetica* ("l'anello $\mathbf{Z}$ dei numeri interi è un dominio a fattorizzazione unica"). Esistono in $\mathbf{Z}$ infiniti elementi irriducibili (=pri-mi). Esistenza di *m.c.m.* in $\mathbf{Z}$, relazione con *M.C.D.*

Equazioni diofantee in $\mathbf{Z}$; semplificazioni, criterio di risolubilità, metodo risolutivo.

Congruenza modulo n in $\mathbf{Z}$; definizione, descrizione del quoziente $\mathbf{Z}_n$, compatibilità con somma e prodotto. Somma e prodotto in $\mathbf{Z}_n$; definizione, proprietà. Criteri di divisibilità tra numeri interi.

Equazioni congruenziali lineari (in $\mathbf{Z}$), equazioni modulari (in $\mathbf{Z}_n$); semplificazioni, criterio di risolubilità, metodi di soluzione. Il gruppo $U(\mathbf{Z}_n)$ degli invertibili in $\mathbf{Z}_n$, criterio di invertibilità; la funzione di Eulero. Calcolo di potenze in $\mathbf{Z}_n$: generalità, il *Piccolo Teorema di Fermat*, il *Teorema di Eulero*.

Sistemi di equazioni congruenziali (lineari); sistemi in forma cinese. Il *Teorema Cinese del Resto* (formulato per sistemi di congruenze e formulato in termini di anelli di interi modulari e loro prodotti diretti).

6 – GRUPPI

Gruppi e loro (omo)morfismi. Ordine di un gruppo. Il *Teorema di Cayley per Gruppi*: ogni gruppo G si immerge nel gruppo delle permutazioni su G.

Sottogruppi; criteri perché un sottoinsieme di un gruppo sia un sottogruppo. Intersezione e unione di una famiglia di sottogruppi. Il sottogruppo generato da un sottoinsieme: esistenza e descrizione.

Gruppi e sottogruppi ciclici. L'ordine di un elemento in un gruppo. Il *Teorema di Struttura dei Gruppi Ciclic*i (isomorfismo con $\mathbf{Z}$ o con $\mathbf{Z}_n$); classificazione dei gruppi ciclici. Biiezione tra i sotto-gruppi di un gruppo ciclico finito e i divisori del suo ordine. I generatori di un gruppo ciclico.

Equivalenze (destre e sinistre) in un gruppo associate ad un sottogruppo. Classi laterali di un sottogruppo; cardinalità delle classi laterali; indice di un sottogruppo. Il *Teorema di Lagrange* per gruppi finiti, e conseguenze: il *Teorema di Eulero*, il *Piccolo Teorema di Fermat*. Il sottogruppo associato ad una equivalenza compatibile in un gruppo; sottogruppi normali. Biiezione tra equivalenze compatibili e sottogruppi normali. Gruppi quoziente (rispetto a equivalenze compatibili).

Immagine e nucleo di un morfismo di gruppi. Un morfismo tra gruppi è iniettivo, risp. suriettivo, $\Leftrightarrow$ ha nucleo banale, risp. ha immagine totale. I sottogruppi normali di un gruppo G sono tutti e soli i nuclei dei morfismi di gruppo con dominio G.

Il *Teorema Fondamentale di Omomorfismo per Gruppi*.

Le corrispondenze tra sottogruppi (o sottogruppi normali) del dominio e del codominio tramite un morfismo di gruppi; il caso suriettivo. Sottogruppi e sottogruppi normali di un gruppo quoziente.

7 – AZIONI DI GRUPPI, *G*-SPAZI

Azioni/rappresentazioni di un gruppo su un insieme: *G*-insiemi (o "*G*-spazi"). *G*-orbite, stabilizzatori, punti fissi; azioni fedeli, azioni transitive, *G*-spazi omogenei. Relazione tra orbita e stabilizzatore di un punto in un *G*-spazio. Azioni indotte (sui sottoinsiemi, sulle partizioni, ecc.). Azioni di un gruppo su sé stesso: sinistra, destra, per coniugazione. Centralizzante di un elemento in un gruppo.

Equazione delle Classi in un gruppo finito. Il *Teorema di Burnside*.

Il gruppo simmetrico $\mathcal{S}(X)$ delle permutazioni di un insieme X; il gruppo simmetrico $\mathcal{S}_n$ su n elementi. Permutazioni cicliche; esistenza e unicità della fattorizzazione di una permutazione in prodotto di cicli disgiunti; ordine di una permutazione. Ordine e lunghezza di una permutazione ciclica; calcolo dell'ordine di una permutazione generica. Fattorizzazione di una permutazione in prodotto di trasposizioni; parità di una permutazione; il sottogruppo alterno $\mathcal{A}_n$. Partizioni di n. Coniugazione nel gruppo $\mathcal{S}_n$. Classi coniugate in $\mathcal{S}_n$: biiezione con le partizioni di n.

Il gruppo diedrale $\mathcal{D}_n$ su n elementi: definizione come gruppo di automorfismi del grafo ciclico con n vertici. Calcoli in $\mathcal{D}_n$, formule fondamentali per rotazioni e riflessioni.

8 – ANELLI

Anelli; casi speciali: commutativi, unitari, integri; corpi, campi. Anelli numerici; anelli di matrici; anelli di polinomi (o di serie), o di polinomi (o serie) di Laurent, o di funzioni razionali. Prodotto diretto di anelli; anelli di funzioni. L'anello degli endomorfismi di un gruppo abeliano.

Sottoanelli di un anello; criteri per riconoscere un sottoanello. Unione e intersezione di sottoanelli. Sottoanelli generati da un sottoinsieme: esistenza e descrizione.

(Omo)morfismi tra anelli. Immagine e nucleo di un morfismo tra anelli. Un morfismo tra anelli è iniettivo, risp. suriettivo, $\Leftrightarrow$ ha nucleo banale, risp. ha immagine totale.

Il *Teorema di Cayley per Anelli*: il caso speciale degli anelli unitari.

Relazioni compatibili in un anello; anelli quoziente (rispetto a equivalenze compatibili). Ideali sinistri/destri/bilateri. Biiezione tra equivalenze compatibili e ideali (bilateri). Gli ideali (bilateri) di un anello A sono tutti e soli i nuclei dei morfismi di anello con dominio A. Ideali sinistri/destri/bilateri generati da un sottoinsieme: esistenza e descrizione. Ideali principali, anelli a ideali principali.

Il *Teorema Fondamentale di Omomorfismo per Anelli*. Le corrispondenze tra sottoanelli o ideali (sinistri, o destri, o bilateri) del dominio e del codominio tramite un morfismo di anelli; il caso suriettivo. Sottoanelli e ideali (sinistri, o destri, o bilateri) di un anello quoziente.

Il campo dei quozienti di un dominio. *Esempi:* numeri razionali, funzioni razionali..

BIBLIOGRAFIA

Materiale didattico vario disponibile su www.mat.uniroma2.it/~gavarini/page-web_files/mat-didat.html

Piacentini Cattaneo G. M., "Algebra", ed. Decibel-Zanichelli, Padova, 1996

Campanella G., "Appunti di Algebra 1" - "Appunti di Algebra 2"

Herstein I. N., "Algebra", Editori Riuniti University Press, Roma, 2010

==========